UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE NEW YORK TIMES COMPANY, NICHOLAS CONFESSORE, and GABRIEL DANCE,

Plaintiffs,

-v-

FEDERAL COMMUNICATIONS COMMISSION,

Defendant.

18 Civ. 8607 (LGS)

DEFENDANT FEDERAL COMMUNICATIONS COMMISSION'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel.: (212) 637-2721
Fax: (212) 637-2686
Email: tomoko.onozawa@usdoj.gov

TOMOKO ONOZAWA
Assistant United States Attorney, *Of Counsel*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Defendant Federal Communications Commission ("FCC"), by its attorney, Geoffrey S. Berman, United States Attorney for the Southern District of New York, respectfully submits this memorandum of law in support of its motion for summary judgment pursuant to Fed. R. Civ. P. 56 Rule 56 of the Federal Rules of Civil Procedure.

PRELIMINARY STATEMENT

Plaintiffs The New York Times, Nicholas Confessore, and Gabriel Dance ("Plaintiffs") commenced this FOIA action to compel FCC to release from its Electronic Comment Filing System, server logs related to public comments posted to FCC Docket No. 17-108[1] from April 2017 to June 2017. The information sought by Plaintiffs' FOIA request, as amended multiple times, however, is exempt from disclosure because their request—depending on the type of server logs implicated by the request—amounts to: (1) a demand that FCC essentially conduct research to conceptualize and develop new technical means of extracting data from server logs in a manner the FCC does not presently do or know how to do; or (2) a demand that FCC create a new record that does not exist. FOIA does not mandate agencies to undertake these tasks to satisfy a FOIA request.

Separately, the information sought by Plaintiffs' FOIA request is also exempt from disclosure under FOIA because it seeks the disclosure of the IP addresses of every individual who submitted a public comment on the agency's Electronic Comment Filing System. Because IP addresses in the FCC's server logs are information about public commenters in "personnel and medical files and similar files," disclosure of their IP addresses would constitute a clearly unwarranted invasion of their privacy, and Plaintiffs cannot meet their burden of showing that an overriding public interest warrants disclosure, the IP addresses sought by Plaintiffs' request

[1] *See In the Matter of Restoring Internet Freedom*, WC Docket No. 17-108, Notice of Proposed Rulemaking, 32 F.C.C. Rcd. 4434 (2017).

should be denied under FOIA Exemption 6. Accordingly, this Court should grant summary judgment in FCC's favor.

BACKGROUND

A. The FCC's Electronic Comment Filing System

The FCC is an independent federal agency with the authority to regulate interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and territories of the United States. *See generally* The FCC's Mission, *available at* https://www.fcc.gov/about/overview. Like all federal agencies, the FCC engages in "notice and comment" rulemaking processes in accordance with the Administrative Procedure Act, 5 U.S.C. § 553(b), under which the FCC gives the public notice of proposed regulations and seeks public comment. *See generally* Rulemaking Process, *available at* https://www.fcc.gov/about-fcc/rulemaking-process. The Electronic Comment Filing System ("ECFS") is an information system that serves as the FCC's repository for public comments and other materials submitted in the course of the FCC's rulemaking process and other docketed proceedings. *See* Declaration of Erik Scheibert, dated March 14, 2019 ("Scheibert Decl.") ¶ 5. ECFS allows members of the public to comment electronically on FCC proceedings and to access comments other parties have filed. *Id.* ECFS is therefore designed as an open, public-facing system that has been configured to be easily accessed and used by any member of the public interested in participating in or learning about an FCC proceeding. *Id.* ECFS is designed to accept data from the public in large volumes and in a wide variety of formats, and to manage large spikes in traffic that the system experiences during high-profile proceedings. *Id.*

The FCC's Information Technology ("IT") staff built and currently operates and maintains ECFS. *Id.* ¶ 6. At all times relevant to this FOIA case, ECFS was an application built on cloud-computing infrastructure, and consisted of a number of virtual servers and other devices operating within a "virtual private cloud." *Id.* This "virtual private cloud" is separated from the public Internet by firewalls and other security measures. *Id.*

Any member of the public can access ECFS to submit comments or to search for and review other users' comments via one of two ways from the Internet. *Id.* ¶ 7. A user can access ECFS through the human user interface located at the following Uniform Resource Locator ("URL"): https://www.fcc.gov/ecfs. *Id.* A user can also access ECFS through an application programming interface ("API") located at the following URL: https://publicapi.fcc.gov/ecfs. *Id.* The API allows users to extract information from and/or submit comments to ECFS in larger volumes and at faster rates than the human user interface allows. *Id.*

ECFS gives users the option either to file comments with supporting documents ("Standard Filings") or to submit their comments via an online form ("Express Filings"). *Id.* ¶ 8. For Standard and Express filings, ECFS requires users to identify the proceeding on which they are commenting and to provide their names and postal addresses. *Id.* The Standard and Express filing forms include the following notice: "You are filing a document into an official FCC proceeding. All information submitted, including names and addresses, will be publicly available via the web." *Id.*

ECFS processes users' computerized requests to submit or review comments in a variety of ways. *Id.* ¶ 9. A "request" means any of the common "client" request methods defined by the hypertext transfer protocol ("http"). *Id.* ¶ 9 n.1. The FOIA Request, as originally submitted and as amended, refers to "GET" and "POST" requests. *Id.* A successful GET request will retrieve data from ECFS, while a successful POST request will submit new data into ECFS. *Id.* Common requests for information can be fulfilled by information stored (or "cached") external to the ECFS application by a commercial content delivery network with which the FCC contracts to help manage ECFS web traffic. *Id.* ¶ 9. Other information requests and all requests to submit comments are processed through a series of intermediate application elements (known as "hops") located internally within the ECFS application, before the requests reach the internal FCC servers in which ECFS content is stored and processed (the ECFS "application" and "database" servers). *Id.*

These internal hops include software, known as "load balancers," that distributes user requests among the computing resources available in ECFS. *Id.* ¶ 10. The hops include web servers that process and respond to user web requests, and proxy servers that organize and filter the requests. *Id.* To allow these application elements to communicate with each other and to process user requests, each of these internal ECFS servers is assigned a private Internet Protocol ("IP") address. *Id.* Processing a single request through multiple hops will take a certain period of time, usually less than a second, but sometimes longer in high traffic periods. *Id.*

The FCC has a strong security interest in protecting ECFS's internal configuration from public disclosure. *Id.* ¶ 11. Publicly disclosing the internal IP addresses that link various ECFS components together will give attackers a roadmap through the ECFS and threaten the confidentiality, integrity or availability of the information in the ECFS database and the system itself. *Id.* Attackers can also use the internal IP addresses to access the system elements that manage system traffic and process user requests. *Id.* In addition, attackers can delete or alter information in the system, or make the system publicly inaccessible. *Id.* More generally, if internal information about the ECFS system is publicly disclosed, attackers will have valuable information about how the FCC secures and configures its other information systems, including systems operated by the FCC's Enforcement Bureau, its Public Safety and Homeland Security Bureau, and its Office of Inspector General. *Id.*

B. The June 2017 FOIA Request

On or about June 22, 2017, plaintiff Nicholas Confessore ("Confessore"), on behalf of The New York Times, submitted a FOIA request to the FCC, which was assigned FOIA Control No. FCC-2017-000764 ("June 2017 Request"). *Id.* ¶ 12 & Ex. A. The June 2017 Request asked the FCC to:

> [P]rovide the web server logs for comments submitted for Federal Communications Commission docket No. 17-108 between 4/26/17 and 6/7/2017. I would like the logs for requests submitted via both to https://www.fcc.gov/ecfs/filings/ and any submissions through the FCC's API (application programming interface). For each comment, please include the following information: 1) Server logs for both GET and POST requests 2) The date/time stamp of each request 3) The full query including query strings 4) The IP address of the client making the request 5) The browser USERAGENT 6) The following headers when available: Accept, Accept-Encoding, Accept-Language, Connection, Host, DNT, Upgrade-Insecure-Requests, Via, X-Forwarded-For.

Id. The FCC denied the June 2017 FOIA Request by letter dated July 21, 2017, on the grounds that it sought material that was exempt from disclosure pursuant to Exemption (b)(6) of the FOIA. *Id.* ¶ 13 & Ex. B. By letter dated July 25, 2017, The New York Times appealed the FCC's denial. *Id.* ¶ 14 & Ex. C.

Server logs are files that a server automatically generates when it or another system element performs its activities. *Id.* ¶ 16. The data in server logs are not "submitted" by users; they are artifacts of the machine-to-machine communication necessary to execute a request. *Id.* Separate and apart from the FCC's objection to the June 2017 Request on Exemption 6 grounds, that request as drafted presented a practical impossibility for generating responsive records. *Id.* ¶ 15. Although that request sought "web server logs for comments submitted for Federal Communications Commission docket No. 17-108" for a specified time period, ECFS does not have a single set of server logs that comprehensively documents ECFS's activities. *Id.* ¶ 16.

Instead, *multiple* server logs document the activities of the various internal servers and other elements involved in the operations of ECFS. *Id.*

Significantly, ECFS does not assign a unique identifier to incoming requests in order to accurately track the processing of user requests across multiple server log entries. *Id.* If ECFS had such a feature, FCC IT staff could reliably map the processing of a user request throughout the servers, or hops, in the ECFS system. *Id.* Because ECFS lacks such a feature, it is impossible for the FCC to directly and definitively track a public comment in the database back to "the IP address of the client making the request," as sought by the June 2017 Request. *Id.* This is because the data captured in internal server logs typically records only the immediately preceding internal hop, rather than the entire path of the request. *Id.*

To <u>approximately</u> track a single comment back to its original user request, the FCC would have to engage in a painstaking process of working backwards from the date and time the comment appeared in the ECFS database, as opposed to relying on a reliable unique identifier that would attach to and track the request as it progressed through multiple internal hops. *Id.* ¶ 17. The only way the FCC can approximately track a single comment is to laboriously retrace the request's path through the multiple internal hops, as those hops are recorded in multiple server logs, back out to the original request made from the public Internet. *Id.* The retracing process would allow the FCC to identify several requests made close in time to the second the comment appears in the database, and guess which one is the actual originating request. *Id.* However, the FCC cannot directly and conclusively correlate one ECFS request with one ECFS comment. *Id.*

The FCC also determined that several other factors complicated the process for tracking a single comment back to the original user request. *Id.* ¶ 18. In busy periods, for example, ECFS receives thousands of requests a minute, so there can be a large number of requests that correlate very closely in time with a specific comment. *Id.* Time correlation is also complicated by the fact that the individual servers' timestamp mechanisms are not fully synchronized. *Id.* Furthermore, the server logs record user requests for all ECFS dockets, so a POST log entry will not disclose whether the user was posting a comment in FCC Docket No. 17-108 or in another of the hundreds of proceedings that were active in April and May 2017. *Id.*

Separately, the June 2017 Request also created security concerns for the FCC. *Id.* ¶ 19. If the FCC publicly discloses the server logs necessary to trace a submitted comment back to the requester's IP address, it will also end up disclosing the IP addresses of the internal system elements (the hops) through which the request traveled, and compromise the security of the FCC's computer systems. *Id.* ¶¶ 11, 19.

C. The September 2017 and December 2017 Amended FOIA Requests

The FCC and The New York Times engaged in email and telephone communications in an attempt to reach a consensual resolution regarding the FOIA Request. *Id.* ¶ 20. The New York Times amended its FOIA Request through e-mail correspondence on September 22, 2017 ("September 2017 Request"), and a letter on December 21, 2017 ("December 2017 Request"). *Id.* ¶ 21; Exs. D & E. The amended FOIA Requests reduced the number of server log elements that The New York Times sought. *Id.* Specifically, the September 2017 Request eliminated the following header information from the original FOIA Request: Accept, Accept-Encoding, Accept-Language, Connection, Host, DNT, Upgrade-Unsecure-Requests, Via. *Id.* ¶ 21 & Ex. D. The December 2017 Request further eliminated the "X-Forwarded-for" header and the full query, including query strings, from the June 2017 Request. *Id.* ¶ 21 & Ex. E. The December 2017 Request therefore sought four elements: "For each comment on docket 17-108…the comment; the originating IP address; the date and time stamp, and the User-Agent header."

Despite these modifications, however, the December 2017 Request still required the FCC to correlate a submitted comment with a specific ECFS request. *Id.* ¶ 21.

As described in the Scheibert Declaration, the manner in which ECFS system elements are configured makes the requested correlation between specific comments and ECFS requests highly complicated and burdensome, even if it is possible to do the correlation in the first place. *Id.* ¶¶ 16–18. Therefore, The New York Times's attempts to narrow its June 2017 Request did not meaningfully reduce the technical difficulty of correlating a comment to its originating ECFS request. *Id.* ¶ 21. In addition, the amended requests still sought the intermediate logs necessary to trace a submitted comment back to the requester's IP address, and thus did not address any of the FCC's security concerns over disclosing sensitive information about the FCC's network architecture. *Id.* ¶¶ 11, 19, 21.

By letter dated January 29, 2018, the FCC transmitted a supplemental response to its July 2017 denial of The New York Times's June 2017 Request. *Id.* ¶ 22 & Ex. F. In that letter, the FCC stated that the records sought by the June 2017 Request is exempt from disclosure because IP addresses are protected by FOIA Exemption 6. *Id.* The FCC also stated that the requested server logs were subject to withholding under FOIA Exemption 7(E) because revealing the logs would reveal "information about how the Commission protects the security of the ECFS and its other information assets." *Id.* By letter dated February 26, 2018, The New York Times appealed the FCC's supplemental denial. *Id.* ¶ 23 & Ex. G.

D. The May 2018 and August 2018 Amended FOIA Requests

By letter dated May 7, 2018, The New York Times amended Confessore's FOIA Request ("May 2018 Request"). *Id.* ¶ 24 & Ex. H. The May 2018 Request stated The New York Times's understanding of the configuration of the ECFS server logs, and the obstacle this created to the FOIA Request. The letter stated:

> The FCC can't definitively link [the user IP address] to [the User-Agent header] because i) there's no unique identifier recorded in each set of logs, and ii) it takes time to flow through each layer, so the timestamps for a single comment might be slightly different between the two sets of logs.

Id. ¶ 24 & Ex. H, at 2. The May 2018 Request also acknowledged the FCC's security concerns about disclosing the internal IP addresses and agreed that the FCC could withhold those addresses. *Id.*

The May 2018 Request narrowed The New York Times's prior FOIA request to seek:

> [L]ogs from the FCC's web servers handling requests to www.fcc.gov/ecfs/filings and the FCC's API between April 26, 2017 and June 7, 2017, with any non-originating IP addresses removed using a method like the one described above, but retaining any User-Agent headers and originating IP addresses, along with their respective timestamps. Additionally we're requesting the comments, names and timestamps in ECFS submitted between the same dates.

Id. at 3.

The May 2018 Request thus sought at least two log files: one log showing the originating IP addresses and another log showing the "User-Agent" information of ECFS requests made from April 26, 2017, to June 7, 2017. *Id.* ¶ 26 & Ex. H, at 1. The "User-Agent" field in server logs contains specific information about a user's computer system, such as the operating system, operating system version, browser version, the browser platform, and the user's language settings. *Id.* ¶ 27. Additionally, to address the FCC's concern that revealing the IP addresses of its internal servers will pose a security risk, the May 2018 Request asked the FCC to employ a "find-and-replace" process to replace these internal IP addresses with newly-created identifiers which would show that the two log files were associated with each other. *Id.* ¶ 26 & Ex. H, at 2. For example, if a server's IP address is "100.1.1.1," or "100.1.1.2," under The New York Times's May 2018 Request, FCC will be required to find and replace that address with the unique identifier "A-1," or "A-2," respectively. *Id.* ¶ 26 & Ex. H, at 2–3.

In its May 2018 Request, The New York Times explained that it will use this information to perform a "statistical analysis of the data." *Id.* ¶ 27 & Ex. H, at 2. The FCC understands this to mean that The New York Times will attempt to correlate a submitter's IP address to the submitter's comments in FCC Docket No. 17-108 by using both the time stamp and the unique identifier ("A-1," "A-2," etc.). Because the User-Agent field contains specific information relating to a user's computer system, it will help someone identify particular users and distinguish between two users who share the same IP address. *Id.* Accordingly, the FCC also understands that The New York Times will attempt to use the user's originating IP address and the "User-Agent" field to further distinguish among users, especially those who share the same IP address—*i.e.,* two users who work at one facility. *Id.*

By letter dated August 31, 3018, The New York Times modified the FOIA Request again ("August 2018 Request"). *Id.* ¶ 28 & Ex. I. The August 2018 Request sought:

> [L]ogs from the FCC's web servers handling requests for docket no. 17-108 to www.fcc.gov/ecfs/filings/ and the FCC's API between April 26, 2017 and June 7, 2017, with any non-originating IP addresses removed using a method like the one described in the May 7, 2018 letter, but retaining any User-Agent headers and originating IP addresses along with their respective timestamps.

Id. Ex. I, at 1. Other than eliminating that portion of the May 2018 Request which sought "comments, names, and timestamps in ECFS for comments submitted between the specified dates," *id.*, the August 2018 Request was identical to the May 2018 Request. *Id.* ¶ 28. The August 2018 modification had no practical effect on addressing the burdens and concerns that FCC raised in prior discussions with The New York Times, because the "comments, names, and timestamps" for comments submitted to ECFS are already publicly available, as the May 2018 Request acknowledged. *See* Ex. H, at 1 (noting that the originating IP address and the User-Agent header that were sought by the FOIA Request "are not included in the public ECFS data").

On or about September 20, 2018, Plaintiffs filed the instant Complaint against the FCC, seeking an order compelling the FCC to provide Plaintiffs with the requested records [Dkt. No. 1].

ARGUMENT

A. Summary Judgment Standard

FOIA was enacted to "ensure an informed citizenry, . . . needed to check against corruption and to hold the governors accountable to the governed." *NLRB. v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). At the same time, FOIA exempts nine categories of information from disclosure, while providing that "[a]ny reasonably segregable portion of a record shall be provided . . . after deletion of the portions which are exempt under this subsection." 5 U.S.C. § 552(b). FOIA thus "calls for broad disclosure of [g]overnment records, while maintaining a balance between the public's right to know and the government's legitimate interest in keeping certain information confidential." *Associated Press v. U.S. Dep't of Justice*, 549 F.3d 62, 64 (2d Cir. 2008) (citations and internal quotation marks omitted); *Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice*, 331 F.3d 918, 925 (D.C. Cir. 2003).

Summary judgment pursuant to Fed. R. Civ. P. 56 Federal Rule of Civil Procedure 56 is the procedural vehicle by which most FOIA actions are resolved. *See, e.g.*, *Grand Cent. P'ship, Inc. v. Cuomo*, 166 F.3d 473, 478 (2d Cir. 1999); *Carney v. U.S. Dep't of Justice*, 19 F.3d 807, 812 (2d Cir. 1994). "Affidavits or declarations . . . giving reasonably detailed explanations why any withheld documents fall within an exemption are sufficient to sustain the agency's burden." *Id.* (footnote omitted); *see also Halpern v. Federal Bureau of Investigation*, 181 F.3d 279, 291 (2d Cir. 1999) (same). Although this Court reviews *de novo* the agency's determination that requested information falls within a FOIA exemption, *see* 5 U.S.C. § 552(a)(4)(B); *Halpern*, 181 F.3d at 287, the declarations submitted by the agency in support of its determination are "accorded a presumption of good faith," *Carney*, 19 F.3d at 812 (citation and internal quotation marks omitted). "Ultimately, an agency's justification for invoking a FOIA exception is sufficient if it appears logical or plausible." *New York Times Co. v. U.S. Dep't of Justice*, 872 F. Supp. 2d 309, 315 (S.D.N.Y. 2012) (quoting *Wilner v. Nat'l Security Agency*, 592 F.3d 60, 73 (2d Cir. 2009)).

B. Responding to Plaintiffs' May 2018 and August 2018 FOIA Requests as Written Requires the FCC to Create New Records, Which Cannot Be Compelled Under FOIA

The New York Times's May 2018 and August 2018 Requests seek at least two server logs, in which one type of information that appears in every server log—the internal IP addresses of the FCC's servers—has been replaced by a new, unique identifier, created by the FCC solely to comply with this request. Scheibert Decl. ¶¶ 26, 28; Ex. H, at 2–3, Ex. I, at 1. The New York Times has explained that the unique identifiers are necessary to allow it to match two pieces of information—a user's originating IP address and User-Agent header—that reside in separate server logs.[2] The New York Times proposes that the FCC employ a "find-and-replace" process to replace the internal server IP addresses in the requested server logs with newly-created identifiers which would show that two log files are associated with each other. *Id.* ¶¶ 26, 31; Ex.

[2] The FCC understands that the May and September 2018 FOIA Requests were based on a representation previously conveyed by the FCC to The New York Times, that there is no single server log in ECFS that contains both a user's originating address and User-Agent file. *See* Scheibert Decl. ¶ 29 & Ex. H, at 1. However, FCC subsequently determined as it was finalizing work on and supporting this memorandum that ECFS does have one server with a log, known as the "API proxy server log," that includes both a user's originating IP address and User-Agent file. *See* Scheibert Decl. ¶ 29. As set forth in Section C of this brief, however, releasing the API proxy server log in a manner consistent with the requirements in The New York Times's May 2018 and August 2018 Requests still entails conducting research outside the scope of FOIA and the release of information protected by FOIA Exemption 6. However, to the extent The New York Times believes that the API proxy server log described in Section C of this brief is not fully responsive to its amended FOIA Requests and instead seeks the same information through multiple server logs, this Section B explains how releasing multiple logs in the format proposed by The New York Times's May and August 2018 Requests is also not required under FOIA.

H, at 2–3. If, for example, a server's IP address is "100.1.1.1," or "100.1.1.2," The New York Times's proposal will require the FCC to find and replace each and every internal IP address with a unique identifier called "A-1," or "A-2," respectively. *Id.* ¶ 26. In reality, this proposal is not a mere "find-and-replace" process, and replacing existing server addresses with unique identifiers requires the creation of a new record that neither exists nor is maintained as part of the FCC's operations. *Id.* ¶¶ 31–33.

FOIA does not permit courts to compel an agency to produce anything other than responsive, non-exempt records. *See* 5 U.S.C. § 552(a)(4)(B) (district court "has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld" from plaintiff). Once an agency establishes that information falls within a FOIA exemption, it cannot be compelled to produce that information, even in an altered or modified form. *See, e.g., Kissinger* v. *Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 152 (1980) ("The Act does not obligate agencies to create or retain documents."); *NLRB* v. *Sears, Roebuck & Co.*, 421 U.S. 132, 162 (1975); *ACLU v. Dep't of Justice*, 681 F.3d 61, 71 (2d Cir. 2012) ("if the Government altered or modified the [requested document] . . . the Government would effectively be 'creating' documents—something FOIA does not obligate agencies to do").

The work entailed in responding to the May and August 2018 FOIA Requests as drafted would amount to the creation of new records. To create these new records, FCC technical specialists will first have to design and write a computer program ("a script") capable of analyzing each element of the data rows contained in the responsive server logs, and then extract and modify the requested elements (*e.g.*, the internal IP addresses) from these logs. *Id.* ¶ 32. There are significant technical hurdles to developing such a script. *Id.* For example, due to the cloud-based architecture of ECFS, in which IP addresses are dynamically assigned to different servers as supply and demand for the service changes, the script will need to be tailored to properly replace *each* version of that server's IP address with a unique identifier. *Id.* ¶ 33. Once written, FCC technical specialists will need to test and manually check each script to ensure that it operates as intended, and validate it using multiple data sets. *Id.* The entire process of developing and testing the script to create the requested record will likely take over a week of IT staff time. *Id.* FOIA simply does not require agencies to undertake that burden. *See, e.g., Ctr. for Public Integrity v. FCC*, 505 F. Supp. 2d 106, 114 (D.D.C. 2007) (FOIA request was the impermissible creation of a new record, where "plaintiff's proposal would require the FCC to do more than simply redact portions of the numbers [contained in the requested records]," but would require the agency "to replace the redacted numbers with the new numbers").

C. Restricting Even A Single Server Log To Comments In A Single Proceeding, As Plaintiffs Request, Would Require FCC to Research and Develop the Technical Means of Extracting the Server Log Data

Although the FCC's Office of General Counsel previously believed that the only manner in which it could respond to The New York Times's FOIA Request would involve releasing and correlating multiple server logs, FCC recently determined that ECFS contains one server with a log, known as an "API proxy server log," that includes both a user's originating IP address and User-Agent header. *Id.* ¶ 29. However, the API proxy server log is not limited to nor organized in a way that separates or distinguishes among requests associated with a particular FCC proceeding. *Id.* The API proxy server log also does not identify the FCC proceeding to which an ECFS request is ultimately directed. *Id.* Instead, the API proxy server log contains other types of ECFS requests besides requests to post comments, such as requests to download comments. *Id.*

The FCC understood New York Times's FOIA request, as it evolved from its initial June 2017 submission date to its latest amendment in August 2018, to seek server log entries specifically related to FCC Docket No. 17-108. *See, e.g.,* June 2017 Request ("[p]lease provide the web server logs for comments submitted for [FCC] Docket No. 17-108"), *id.* Ex. A, at 1; December 2017 Request (seeking records "[f]or each comment on docket number 17-108"), *id.* Ex. E, at 2; August 2018 Request (referring to "the FCC's web servers handling requests for docket no. 17-108") *id.* Ex. I, at 1. Because the submission data on the API proxy server log is not limited to a specific proceeding, for the FCC to separate out comments for a particular proceeding, like FCC Docket No. 17-108, the FCC would have to attempt to identify comments based on time-stamp matches between individual ECFS entries and the API proxy server log. Scheibert Decl. ¶ 17. That is, FCC staff would need to identify those ECFS comments in FCC Docket No. 17-108, and try to match those comments to the server log with the corresponding IP address and User-Agent heading of the commenter. *Id.* ¶¶ 17, 30. This is ultimately unreliable because it is impossible to definitely establish such a match based on time stamp information. *Id.* During low-volume periods, where few comments are being filed every minute, it may be possible to link a particular entry in the server log to a given public comment in ECFS. However, during busy periods, ECFS receives thousands of requests a minute, and there can be a large number of requests that correlate very closely in time with a specific comment, making it nearly impossible to identify with certainty which server log entry corresponds with which public comment. *Id.* ¶ 18. Moreover, the individual servers' timestamp mechanisms are not fully synchronized. *Id.*

Attempting such a matching and sorting process would require the FCC to create and test a new program, or script.[3] The creation of a program is no mere database search, as contemplated by FOIA, but rather a creative research task, including the exercise of judgment and analysis. *Id.* ¶ 30. For example, the script's programmer would need to need to make judgments about which server log entries best match comments, based on the time gap between entries. *Id*. The programmer would also need to exercise judgment about what degree of statistical confidence is optimal, and how best to achieve that end. *Id.*

This type of programming goes far beyond the type of search required by FOIA, such as running a query on a database. Indeed, the server logs are not a database at all, but rather a long and unwieldy list of various data. *Id.* In essence, The New York Times's May 2018 and August 2018 Requests are an implied question which asks FCC to show or tell which originating user IP addresses submitted comments to Docket No. 17-208 during a certain period. The only way that FCC can answer that question requires it to design and test a script that will obtain the requested data within a subjectively-determined level of statistical confidence in the desired result. *Id.* The FCC is not required to "answer questions disguised as a FOIA request," *Hudgins v. IRS*, 620 F. Supp. 19, 21 (D.D.C. 1995), nor to "conduct research on behalf of private citizens." *Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 159, n.2 (1980). Nor is the FCC required "by FOIA or any other statute, to dig out all the information that might exist, in whatever form or place it might be found, and to create a document that answers plaintiff's question." *Frank v. U.S. Dep't of Justice*, 941 F. Supp. 4, 5 (D.D.C. 1996). *See id.* (plaintiff's FOIA request to DOJ, seeking *inter alia*, "the number of Special Assistant United States

[3] The script-writing and testing process described herein, *see also* Scheibert Decl. ¶ 30, would also apply if The New York Times is seeking to compel the FCC to release multiple server logs specific to FCC Docket No. 17-108, as described in Section B, *infra*.

Attorneys that were state and local prosecutors during the first three months of 1988," was improper because "FOIA provides access to existing records but does not establish a research service").

D. The IP Addresses and User-Agent Headers Sought By Plaintiffs' May and August 2018 FOIA Requests Are Exempt From Disclosure Under FOIA Exemption 6

In addition, the FCC properly withheld the records sought by Plaintiffs' May and August 2018 Requests because the IP addresses and User-Agent fields contained in the requested server logs apply to all users who made requests to ECFS, and thus qualify for protection under FOIA Exemption 6.

Under FOIA Exemption 6, an agency may withhold "personnel and medical files and similar files" when disclosing such information "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). Exemption 6 serves to "protect individuals from the injury and embarrassment that can result from the unnecessary disclosure of personal information." *Wood v. FBI*, 432 F.3d 78, 86 (2d Cir. 2005) (quoting *U.S. Dep't of State v. Washington Post Co.*, 456 U.S. 595, 599 (1982)). In assessing an agency's withholding of information under Exemption 6, this Court must undertake a two-part inquiry to: (1) determine "whether the records at issue are likely to contain the type of personal information that would be in a medical or personnel file"; and (2) to "balance the public's need for the information against the individual's privacy interest to determine whether the disclosure of the names would constitute a 'clearly unwarranted invasion of personal privacy.'" *Id.* (citations omitted).

For the first prong of the analysis, the Second Circuit has observed that the "phrase 'similar files' sweeps broadly and has been interpreted by the Supreme Court to mean 'detailed Government records on an individual which can be identified as applying to that individual.'" *Cook v. Nat'l Archives & Records Admin.*, 758 F.3d 168, 174 (2d Cir. 2014) (quoting

Washington Post Co., 456 U.S. at 602). Accordingly, "'the protection of an individual's right of privacy' which Congress sought to achieve by preventing 'the disclosure of [information] which might harm the individual,'. . . surely was not intended to turn upon the label of the file which contains the damaging information." *Washington Post Co.*, 456 U.S. at 601 (quoting H.R. Rep. No. 89–1497, at 2418, 2428 (1966)). A wide range of documents beyond personnel or medical files therefore have been deemed "similar files" for purposes of meeting the first prong of the Exemption 6 analysis. *See Seife v. U.S. Dep't of State*, 298 F. Supp. 3d 592, 624 (S.D.N.Y. 2018) (emails, proposed talking points, draft opening statements, and draft rollout schedules are "similar files" under Exemption 6); *Forsythe v. U.S. Nat'l Labor Rel. Bd.*, 14 CV 3127, 2016 WL 1165897, at *6 (E.D.N.Y. Feb. 16, 2016) (administrative investigative records are "similar files" under Exemption 6); *Carter, Fullerton & Hayes LLC v. Federal Trade Comm'n*, 520 F. Supp. 2d 134, 144–45 (D.D.C. 2007) (consumer complaints filed with FTC containing their names, addresses, and telephone numbers are "similar files" under Exemption 6 "[s]ince each piece of information withheld applies to specific individuals").

Here, the FCC correctly concluded that an individual's IP address is protectable under FOIA Exemption 6. Like a phone number or mailing address, an IP address can be linked, in conjunction with other information, to a particular computer or individual. *See* Scheibert Decl. ¶ 35. Even though The New York Times is no longer asking the FCC to produce ECFS comments, its request still risks an invasion of personal privacy by revealing IP addresses. The New York Times itself has stated that it will perform an analysis aimed at linking information provided by the FCC's FOIA response to specific ECFS comments, which are publicly available and include the names and postal addresses entered by members of the public who submitted comments. *Id.* ¶ 36; Ex. H, at 2. Thus, if the agency produces personal IP addresses with the time stamp of a user's request, there is a substantial possibility that The New York Times or any member of the public could match at least some of those IP addresses with individual commenters who made submissions to ECFS during the requested period, by looking up the public comments posted to FCC Docket No. 17-108. Scheibert Decl. ¶¶ 27, 36. To be sure, it is not possible to definitely match all docket entries to IP addresses, as explained above. But the ability to do at least some matching is the foundational premise for The New York Times's request and their stated intention is to perform statistical analysis toward that end. *Id.* ¶ 36; Ex H, at 2. If no such matching were possible, the requested information would be useless, and the fact that The New York Times is pursuing it lends credence to the FCC's belief that the requested production is inconsistent with Exemption 6.

The New York Times's request also runs afoul of Exemption 6 in a second way. The "User-Agent" field in a server log likewise contains specific information about a user's computer system, such as the operating system, operating system version, browser version, the browser platform, and the user's language settings. *Id.* ¶ 27. This too is personal information because the User-Agent field contains specific information relating to a user's computer system, and it will help someone identify particular users and distinguish between two users who share the same IP address. *Id.* The FCC has therefore established that the IP addresses and User-Agent headers in the requested server logs can be identified as applying to specific individuals, and therefore the server logs qualify as "similar files" under that exemption. *Id.* ¶¶ 34–35.

The FCC has also established that the second prong of the Exemption 6 analysis has been met. The disclosure of a user's specific technical information, which is automatically recorded in the FCC's server logs while he or she interacts with ECFS, can constitute an unwarranted invasion of personal privacy, because the requested information can be used to identify, target and potentially harm that user. *Id.* ¶¶ 36–37. Although the FCC informs users that the names and postal addresses provided by commenters as part of their submissions are made public, it does not give ECFS users *any* notice that their log data could be disclosed to third parties. *Id.* ¶ 8. As the Scheibert Declaration explains and, as is at least somewhat familiar to anyone who is afflicted with pop-up digital advertising while browsing the Internet, data sets that combine consumers' "online" and "offline" personal information have a number of applications in the commercial digital marketplace, such as identity verification, fraud detection, and marketing. *Id.* ¶ 36.

Additionally, the privacy risk to ECFS users is not limited to the commercial exploitation of their personal information. Malicious actors who are motivated by their opposition to a commenter's views, financial gain, or some other motive could use this information to commit identity theft or otherwise harm the user. *Id.* ¶ 37. For example, the details disclosed in the User-Agent header information about a given user's system can potentially inform malicious actors as to whether the user is employing an outdated browser or an operating system with a vulnerability. *Id.* By knowing this system information and the associated system's IP address, a malicious actor can potentially exploit that vulnerability. *Id.* Accordingly, the FCC has demonstrated that significant privacy interests warrant disclosure of originating IP addresses under Exemption 6. *Cf., Acosta v. FBI*, 946 F. Supp. 2d 53, 65 (D.D.C. 2013) (agency's "careful and pinpointed redactions of . . . pages that contain only IP addresses and other identifying computer information" were appropriate under FOIA Exemption 7(C) because of "privacy interests" that were "substantial"); *Kortlander v. Bureau of Land Mgmt.*, 816 F. Supp. 2d 1001, 1015 (D. Mont. 2011) (holding that federal employees' names, address, phone numbers, IP addresses, email addresses, Ebay login names and other personal information was protected by Exemptions 6 and 7(C) of FOIA).

Because the disclosure of individuals' IP addresses could result in an invasion of their personal privacy, Plaintiffs, as the FOIA requesters, have the burden of establishing that the disclosure of personal information serves an overriding public interest. *Associated Press v. U.S. Dep't of Justice*, 549 F.3d 62, 66 (2d Cir. 2008). The only cognizable public interest under FOIA is the public's "understanding of the operations or activities of the government." *Long v. Office of Personnel Mgmt.*, 692 F.3d 185, 193 (2d Cir. 2012) (quoting *U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 755 (1989)); *see also Lepelletier v. Federal Deposit Ins. Corp.*, 164 F.3d 37, 46 (D.C. Cir. 1999) ("The only relevant public interest in the FOIA balancing analysis is the extent to which disclosure of the information sought would 'shed light on an agency's performance of its statutory duties' or otherwise let citizens know 'what their government is up to.'") (alterations and citations omitted). Here, Plaintiffs proffer a putative interest in obtaining ECFS server logs, including individual user IP addresses, to "help broaden the public's understanding of the scope of Russian interference in the American democratic system." *See* Compl. ¶ 2. But this asserted interest bears no relation to "open[ing] *agency* action to the light of public scrutiny," *see Dep't of the Air Force v. Rose*, 425 U.S. 352, 372 (1976) (emphasis added), or to "shed[] light on an *agency's* performance of its statutory duties." *Reporters Comm.*, 489 U.S. at 773 (emphasis added). *See, e.g., Associated Press*, 549 F.3d at 66 (plaintiff failed to show how commutation petition submitted by third party to DOJ's Office of the Pardon Attorney, which contained "private, personal information, would in any way shed light on the DOJ's conduct").

In addition, "one factor agencies and courts consider on the public interest side of the equation is the extent to which there are alternative sources of information available that could serve the public interest in disclosure." *U.S. Dep't of Defense v. Fed. Labor Rel. Auth.*, 964 F.2d 26, 29 (D.C. Cir. 1992). If there are "alternative means" for obtaining the information, "the need for enforced disclosure under the FOIA of privacy-implicating information is diminished." *Id.* Plaintiffs' purported interest in "the public understanding of the scope of Russian interference" in FCC Docket No. 17-108 is already being explored in a variety of ways that do not compromise users' privacy. For example, the FCC's Office of the Inspector General,[4] the U.S. Government Accountability Office,[5] the Attorney General of the State of New York,[6] Stanford Law School,[7] and various media outlets[8] have investigated or are investigating the public comment process for FCC Docket No. 17-108. *Cf. Nat'l Archives and Records Admin. v. Favish*, 541 U.S. 157, 175 (2004) (declining to find a public interest where the federal

[4] Federal Communications Commission, Office of the Inspector General, *Memo: Alleged Multiple Denial-of-Service (DDOS) Attacks Involving the FCC's Electronic Comment Filing System (ECFS)* (June 20, 2018), *available at* https://www.fcc.gov/sites/default/files/fcc-oig-roi-ecfs-ddos-08072018.pdf.

[5] *See, e.g.*, Letter from Orice Williams Brown, Managing Director of Congressional Relations, U.S. Government Accountability Office, to the Honorable Frank Pallone, Jr., Ranking Member, Committee on Energy and Commerce, U.S. House of Representatives (Jan. 9, 2018), *available at* https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Pallone_Redacted.pdf.

[6] *See* New York State Office of the Attorney General, Public Notice regarding "Fake Comments," *available at* https://ag.ny.gov/fakecomments.

[7] Ryan Singel, The Center for Internet and Society at Stanford Law School, *What Americans Actually Told the FCC about Net Neutrality Repeal: A state-by-state, district-by-district look at unique comments filed to the FCC in the 2017 repeal proceedings* (October 2018), available at http://cyberlaw.stanford.edu/files/blogs/FilteringOutTheBotsUnique2017NetNeutralityComments1024Update.pdf.

[8] *See, e.g.*, James V. Grimaldi and Paul Overberg, "Millions of People Post Comments on Federal Regulations. Many Are Fake," *Wall Street Journal* (Dec. 12, 2017).

government had investigated the suicide at issue and that “[i]t would be quite extraordinary to say we must ignore the fact that five different inquiries into the . . . matter reached the same conclusion”). Thus, disclosure of that information “would constitute a clearly unwarranted invasion of personal privacy,” 5 U.S.C. § 552(b)(6), and the FCC properly withheld the information under Exemption 6.

CONCLUSION

For the foregoing reasons, the Court should grant summary judgment for defendant the FCCpursuant to Rule 56 of the Federal Rules of Civil Procedure.

Dated: March 14, 2019
New York, New York

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
Attorney for Defendant FCC

By: *\/s/ Tomoko Onozawa*
TOMOKO ONOZAWA
Assistant United States Attorney
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel.: (212) 637-2721
Fax: (212) 637-2686
Email: tomoko.onozawa@usdoj.gov